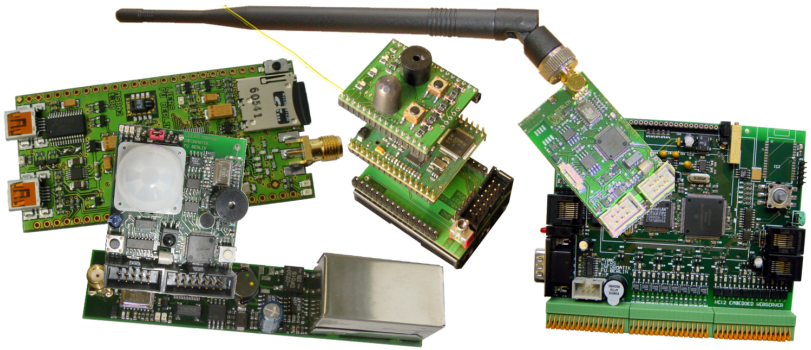


19531 - Telematics

9th Tutorial - IP Model, IPv6, Routing

Bastian Blywis

Department of Mathematics and Computer Science
Institute of Computer Science
06. January, 2011

Outline

1. Evolution of the IP Model
2. IPv6
3. Stateless vs. Stateful Address Auto Configuration
4. Routing
5. Static vs. Dynamic Routing
6. Routing Protocol Types
7. Routing Metrics
8. Routing Table
9. Policy Routing
10. Symmetric Paths
11. Mobile Nodes
12. IPv5

Evolution of the IP Model

Read the Internet draft *Evolution of the IP Model* by Dave Thaler.

1. Host A intends to establish a video conference with host B. Assume that host B can reach host A. Why it is not ensured that A can start the video conference? Discuss your answer with respect to the network layer.
2. What is a multi-homed host?
3. Discuss how addresses, host names, and routing are correlated and if an application programmer should use addresses or names to establish a connection?

Evolution of the IP Model

Host A intends to establish a video conference with host B. Assume that host B can reach host A. Why it is not ensured that A can start the video conference? Discuss your answer with respect to the network layer.

- Reachability may be not symmetric
- Effects caused by attributes of link-layer technologies, and by network-layer
- Unidirectional links (satellite, wireless LANs)
- Network Address Translation

Evolution of the IP Model

What is a multi-homed host?

- Multi-homing provides redundancy and network optimization
- Multi-homed host is connected to the Internet via several IP paths (using different providers)
- Multi-homed (multi-connected) network is connected via several autonomous systems (AS)
- Provider independent (PI) addresses from *Regional Internet Registry* (RIR) instead of provider aggregatable (PA) addresses required

Problems:

- Provider independent addresses prevent route aggregation $\Rightarrow$ larger routing tables
- Provider-bound addresses leave administration to the end system domain
- Upstream links should be physically diverse

Question: How do you realize this with respect to routing and transparent end-host connections? Which source/destination address should you use? What about DNS and Firewalls?

Evolution of the IP Model

Multi-homing variants:

- Single link, multiple IP addresses
- Multiple interfaces, single IP address per interface
- Multiple links, single IP address
- Multiple links, multiple IP address

Evolution of the IP Model

Discuss how addresses, host names, and routing are correlated and if an application programmer should use addresses or names to establish a connection?

IP address management is complex getting more complex:

- Multiple IP addresses per host
- IP address updates
- Addresses required to initialize state in firewalls and NAT devices
- User applications have to resolve names to addresses, ensure reachability, etc
- IP addresses are locators and identifiers (mobility?)

⇒ User applications should use names rather than addresses

Ubillos et. al *Name-Based Sockets Architecture*
Internet Draft **draft-ubillos-name-based-sockets-03**, 2010

1. Discuss the differences of the Internet Protocol version 4 and 6.
2. How long does the IPv6 address space last, when an IPv6 address is assigned every pico-second.
3. How can the two versions of IP coexist?
4. Is ARP required for IPv6 and does ICMP still exist?

IPv6 improvements:

- Addressing and Routing
  - Larger address space
  - Usually multiple addresses per IP-interface
  - Better route aggregation
  - Simple address update for whole networks
- Simplified administration
  - Stateless auto-configuration without DHCP
  - Automated neighbor and router discovery
- Protocol design
  - Lightweight header design to increase processing time
  - Optional extension headers possible
  - IPv6 header has fixed size ⇒ easier to evaluate by routers
  - No header checksums ⇒ error detection on layers 2 and 4 (remark: IPv4 header was only protected by layer 3 checksum)
  - Flow label for virtual connections
  - Anycast addresses
  - No fragmentation (inside the network)
  - Larger maximum size possible (IPv6 Jumbograms), see RFC 2675
- Security
  - Authentication and privacy capabilities

Deering and Hinden *Internet Protocol, Version 6 (IPv6)*
RFC 2460, 1998

Figure: IPv6 Header Format

Extension	Type	Size	RFC
Hop-By-Hop Options	0	variable	RFC 2460
Routing	43	variable	RFC 2460, RFC 3775, RFC 5095
Fragment	44	64 bits	RFC 2460
Authentication Header (AH)	51	variable	RFC 4302
Encapsulating Security Payload (ESP)	50	variable	RFC 4303
Destination Options	60	variable	RFC 2460
No Next Header	59	empty	RFC 2460

Table: IPv6 Extensions (excerpt)

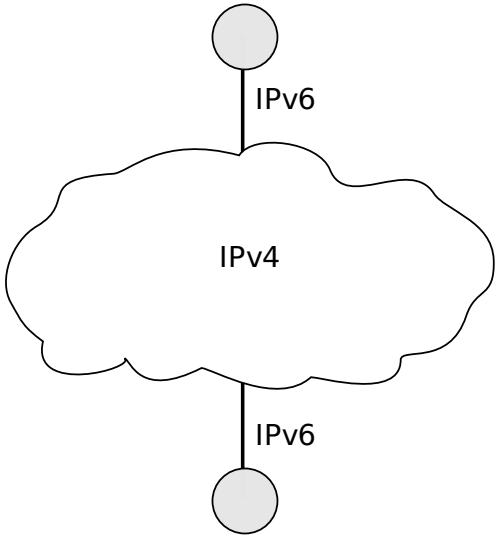
$$
\begin{aligned}
1\,ps &= 10^{-12}\,s && (1)\\
2^{128} \cdot 10^{-12}\,s &\approx 3.4 \cdot 10^{26}\,s && (2)\\
&\approx 1.7 \cdot 10^{19}\text{Jahre} && (3)
\end{aligned}
$$

$\Rightarrow$ 2^{128} should be enough for some time

Note: Of course there are not 2^{128} addresses for hosts but the address pool will last a very long time.

How can these two versions of IP coexist?

- Dual stack techniques, which allow for coexistence of IPv4 and IPv6 at the same host
- Applications have to be migrated successively
- Tunnels between IPv6 domains
  - 6over4, see RFC 2529
  - 6to4, see RFC 1933
  - 6in4, see RFC 4213
  - Teredo tunneling, see RFC 4380
- Address translation gateways



Giligan and Nordmark *Transition Mechanisms for IPv6 Hosts and Routers*
RFC 1933, 1996

Address block	Description	IPv4
::/128	Unspecified	0.0.0.0
::1/128	Loopback	127.0.0.0/8
fe80::/10	Link local	169.254.0.0/16
fc00::/7	Unique local address	
ff00::/8	Multicast	224.0.0.0/4
ff02::1:ff00:0/104	Solicited-node multicast	
::ffff:0:0/96	IPv4 mapped addresses	
2001::/32	Teredo Tunneling	
2002::/16	6to4 addressing	
2001:10::/28	Overlay Routable Cryptographic Hash Identifiers	
2001:db8::/32	Documentation	192.0.2.0/24

Table: Reserved IPv6 Address Blocks

IPv4 mapped addresses

- IPv4 in IPv6 only networks
- ::ffff:0:0/96 prefix
- Upper 80 bits set to zero and next 16 to one
- Last 32 bits represent IPv4 address

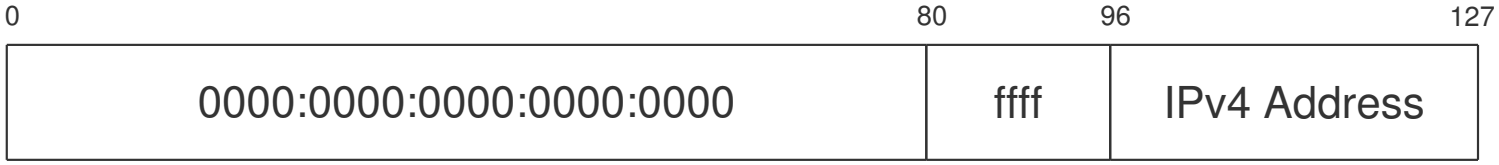


Figure: IPv4 Mapped Address

Is ARP used with IPv6?

- You need a mapping of layer 3 to layer 2 addresses
- Neighbor Discovery Protocol (NDP) substitutes ARP
- NDP is a messaging protocol that specifies communication activities for nodes on the same link (e.g., router discovery, etc.)
- NDP is independent of the link layer protocol
- NDP uses ICMPv6 and multicast to provide the functionality of ARP
- Pure network layer protocol (advantages?)
- NDP functional groups
  - Host-router discovery functions
    - Router discovery
    - Prefix discovery
    - Parameter discovery
    - Address auto-configuration
  - Host-host communication functions
    - Address resolution
    - Next-hop determination
    - Neighbor unreachability detection
    - Duplicate address detection
  - Redirect function

Stateless vs. Stateful Address Auto Configuration

Discuss the difference between *stateless* and *stateful* address configuration!

Stateless vs. Stateful Address Auto Configuration

- Stateful address configuration establishes states to assign addresses, e.g., DHCP
- Stateless configuration allows autonomous address configuration, e.g., IPv6 auto-configuration
  1. Interface assigns a link-local address on activation (tentative address)
  2. Interface sends neighbor solicitation for *Duplicate Address Detection* (DAD)
  3. Interface then listens for *neighbor advertisement*
     - *neighbor advertisement* arrives: link-local address already in use
     - timeout: link-local address is assigned and can be used for communication in local network
  4. Interface listens for *router advertisement* or sends *router solicitation*
  5. Router tells how to proceed
     - Stateful auto-configuration (DHCP)
     - Stateless auto-configuration: interface creates globally-unique address from prefix and link-local address.

Note: DAD is run again, when a global addresses is generated as uniqueness in prefix does not assure uniqueness in another.

Stateless vs. Stateful Address Auto Configuration

Generating a link-local address

1. MAC address, 48 bit:
   00:19:b9:3f:02:f6
2. Conversion to 64bit (EUI-64):
   00:19:b9:ff:fe:3f:02:f6
3. IPv6 notation with inversed universal bit (set to global scope):
   0219:b9ff:fe3f:02f6
4. IPv6 link-local address:
   FE80:0000:0000:0000:0219:b9ff:fe3f:02f6

RFC 3513, Page 8:

> *"The motivation for inverting the "u" bit when forming an interface identifier is to make it easy for system administrators to hand configure non-global identifiers when hardware tokens are not available. This is expected to be case for serial links, tunnel end- points, etc. (. . .)*
>
> *The use of the universal/local bit in the Modified EUI-64 format identifier is to allow development of future technology that can take advantage of interface identifiers with global scope."*

1. Discuss the terms routing and forwarding.
2. Where are the corresponding services implemented in an hierarchical network architecture?
3. Which devices that are between a source and destination node participate in the routing?

- Routing is the process of finding paths in a network between a source and destination (network or application layer)
- Forwarding refers to the relaying of datagrams based on information in a routing table (network layer)
- Routers forward datagrams, switches and bridges to not participate in this routing process

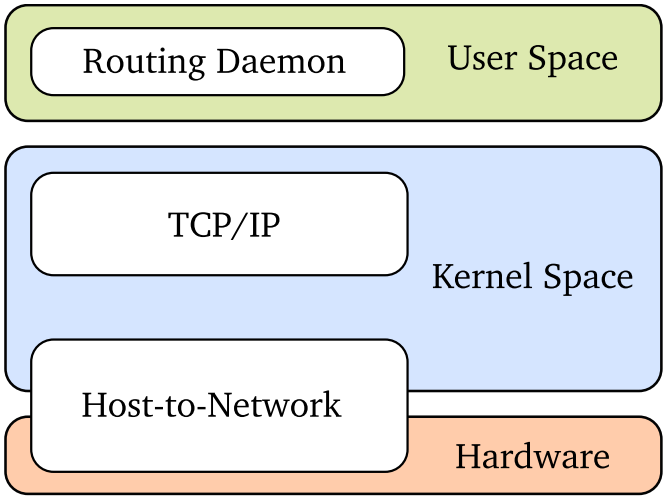


Figure: Routing daemon in user space

Remark: The terms routing and forwarding are often used confused
Remark: In specific scenarios, routing and forwarding can take place in other layers

Static vs. Dynamic Routing

Discuss the advantages and disadvantages of static and dynamic routing.

Static vs. Dynamic Routing

Static Routing:

- Configured by the network administrator
- Does not adapt to changes in the network, e.g., SNR, PDR, or topology
- No overhead due to probe packets, e.g., HELLO messages or management packets
- Optimal path selection possible, routing tree can created in a planed way
- QoS can be considered
- Deterministic routes
- Symmetric routing can be enforced
- Static routing hardly possible in large networks

Static vs. Dynamic Routing

Dynamic Routing:

- Adapts to network changes
- Either network is probed periodically or incoming messages are evaluated
- Routing can be sub-optimal with frequent routes changes
- Even dynamic update of routing information might be too slow to adapt to changes, e.g., in mobile, wireless networks
- QoS criteria harder to ensure

Routing Protocol Types

Classify the different routing approaches. Consider aspects like maintenance, scope, and information distribution.

Routing Protocol Types

- Static vs. dynamic
- Time or route discovery
  - Proactive: periodically discover routes to all destinations
  - Reactive: discover route when it is required
- Flat vs. hierarchical
- Host-intelligent vs. router-intelligent
- Intra-domain vs. inter-domain
- Link-state vs. distance vector

- Link-state routing
  - All nodes discover their neighbors, e.g., using a HELLO protocol
  - All nodes flood their neighborhood information to all other nodes in the network
  - Each node has knowledge of the global topology (but not necessary the same)
  - Each node calculates best next hop for each destination
- Distance vector routing
  - All nodes discover their neighbors, e.g., using a HELLO protocol
  - All nodes sent their neighborhood information/routing table to their neighbors
  - Incoming information (vectors) is incorporated in the routing table
  - Nodes know only best next hop to each destination

Routing Metrics

List metrics that can be used by routing protocols. Discuss suitable application scenarios where these metrics could be used.

Routing Metrics

- Path length / hop count
- Reliability of the path
- Delay
- Throughput
- Maximum Transmission Unit (MTU)
- Load
- Energy
- Political decisions
- Communication cost

Many of these metrics relevant for routing between autonomous systems and when peering separate networks at exchange points

Routing Table

A router has the following routing table:

Destination	Router	Genmask	iface
160.45.0.0	134.14.13.1	255.255.0.0	eth0
160.45.12.0	134.14.14.1	255.255.255.0	eth1
164.13.128.0	74.125.128.1	255.255.128.0	eth2
164.13.0.0	74.125.122.1	255.255.0.0	eth2
default		0.0.0.0	eth0

Over which output interfaces are the datagrams with destination addresses 160.45.1.1, 193.99.144.80, 164.13.130.0, 160.45.12.1 forwarded?

Routing Table

What is policy routing and why is it necessary in todays networks? Have a look at the book *Policy Routing With Linux - Online Edition* by Matthew G. Marsh.

Policy Routing

- Traditional routing is destination-driven, i.e., destination address determines output interface
- Policy routing provides routing capabilities based on further information about a packet
- Used for QoS approaches like IPv4 *Differentiated Services*
- Example Linux kernel:
  - Routing Policy Database (RPDB) with rules
  - Rules can have priorities from 0 through 32767
  - Matching rule determines which routing table to query
  - Up to 256 routing tables (3 are reserved)

Symmetric Paths

Assume that all intra-domain routing follows shortest paths. Why can we not assume symmetric paths within the Internet?

Symmetric Paths

- Intra-domain routing := routing in an autonomous system
- Inter-domain routing := routing between autonomous system
- Routing is performed on intra- and inter-domain level
- Links can be unidirectional and thus the path in the backwards direction can be longer or shorter
- Peering agreements or policy routing can lead to asymmetric paths

Discuss how mobility is considered by IP version 4 and 6 as well as routing in general!

- Short answer: That's what the *Mobile Communications* lecture is for!
- (Slightly) Longer answer:
  - Problem: IP address belongs to a specific network
  - IPv4 does not consider mobility but there are several *Mobile IP* approaches/variants
  - IPv6 addressing makes mobility easier to handle but there are several issues left, e.g., addresses are locators and identifiers

Perkins *IP Mobility Support for IPv4*
RFC 3489, 2002

Johnsan et. al *IP Mobility Support for IPv4*
RFC 3775, 2004

There is IPv4 and IPv6 but what happened to IPv5?!?

- There is no official IPv5
- ST2 was assigned IP version 5 to indicate that the packets are not IPv4 datagrams
- Resource reservation protocol to provide end-to-end real-time guarantees
- Connection-oriented
- ST2 consists of two protocols: ST and SCMP (Stream Control Message Protocol)
- ST2 and IP apply the same addressing schemes
- ST2 messages can be encapsulated in IP packets
- ST2 has been discontinued and focus shifted to IPv6 and RSVP

Delgrossi and Berger *Internet Stream Protocol Version 2 (ST2) Protocol Specification - Version ST2+*
RFC 1819, 1995

The Last Slide™

Thank you for your attention.

Questions?